REMARKS

Claims 1, 2, and 4-35 remain pending in the application. Applicant, by this paper, amends claim 21 and presents claims 1, 2, and 4-35 for reconsideration and allowance.

Discussion of Rejection Under 35 USC §102(e)

Claim 18-20 were rejected under 35 USC §102(e) as allegedly anticipated by U.S. Patent No. 6,101,477 to Hohle et al. (hereinafter Hohle). The Examiner contends that Hohle describes every element of the claims. Applicant respectfully traverses the rejection and requests reconsideration and allowance.

In order for a claim to be anticipated by a reference, the reference must describe each and every element as set forth in the claim, either expressly or inherently, in the single prior art reference. Hohle fails to describe each and every element of claim 18.

Claim 18 recites a method of secure communications between a smart card and a central communications system. The method includes "exchanging secure data through a radio frequency communication channel with the smart card." The method also includes "performing a security function on the data at the central computer system." Applicant respectfully maintains that Hohle fails to describe at least these two claimed elements.

The Examiner alleges that Hohle describes a radio frequency communication channel with the smart card and cites Hohle Col. 3 ll. 31-51. However, this portion of Hohle describes contactless communication techniques that do not utilize a radio communication channel. In the pertinent portion, Hohle states:

> That is, non-contact communication methods may be employed using such techniques as capacitive coupling, inductive coupling, and the like. As is known in the art, capacitive coupling involves incorporating capacitive plates into the card body such that data transfer with a card reader is provided through symmetric pairs of coupled surfaces, wherein capacitance values are typically 10-50 picofarads, and the working range is typically less than one millimeter. Inductive coupling employs coupling

> elements, or conductive loops, disposed in a weakly-coupled transformer configuration employing phase, frequency, or amplitude modulation. *Hohle* Col. 3 ll. 34-45.

Thus, Hohle describes capacitive plate coupling and inductive loop coupling, but does not describe the use of radio frequencies (RF) or a RF communication channel. Indeed, the coupling techniques described in the cited portion of Hohle are usually implemented exclusive of radio frequencies, and there is no indication that the capacitive or inductive coupling is used in conjunction with an RF channel.

The Examiner also alleges that Hohle describes performing a security function at a central computer system, and cites to Hohle, Column 22 ll. 53-58. Although the cited portion of Hohle describes authentication using a message authentication code (MAC), the cited portion does not describe where the authentication is performed. Applicant respectfully contends that Hohle fails to describe performing a security function at a central computer, and instead, describes performing any security functions at the access terminals local to the smart card.

Hohle describes a system in which the access terminals, using software implemented within the terminals, perform any security associated with communicating with the smart card. Hohle states: "Referring again to FIG. 10, access point 15 preferably comprises software which provides a user interface (for example, a graphical user interface) and is capable of executing the appropriate SCOS commands in accordance with the particular transaction being effected." *Hohle* Col 26, ll. 36-40. Hohle further states: "After suitable handshaking between card 100 and the card reader has taken place, and *after the cardholder has been properly authenticated* (i.e., the correct access conditions for updating car preferences EF 810 have been fulfilled), the application program at access point 15 queries the user with a choice of preference codes (for example, those listed in Table 39 above)." *Id.* at ll. 47-53 (*emphasis added*).

Therefore, Hohle described performing the authentication at the local *access points* and not at any central computer system. In fact, Hohle describes how the access terminals can update the card. The access point can send the value to the

appropriate partnering organization. *See id.* at ll. 53-59. Hohle fails to describe any security functions performed by a central computer system. All of the references to operations performed by software refer to operations performed by the access point software. *See generally, Hohle* Col. 26 line 36 through Col. 27 line 45.

Claims 19-20 depend from claim 18 and are believed to be allowable at least for the reason that they depend from an allowable base claim. Thus, Applicant respectfully requests reconsideration and allowance of claims 18-20 because Hohle fails to describe every feature of the claims.

Discussion of Rejection Under 35 USC §103(a)

Claims 1, 2, 4-17, and 29-35 were rejected under 35 USC §103(a) as allegedly unpatentable over Hohle in view of U.S. Patent No. 5,745,571 to Zuk (hereinafter Zuk). Additionally, claims 21-28 were rejected under 35 USC §103(a) as allegedly unpatentable over Hohle in view of U.S. Patent No. 6,226,74 to Murphy et al. (hereinafter Murphy).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be reasonable expectation of success. Finally, the prior art reference, or references when combined, must teach or suggest all of the claim limitations.

There is no motivation to combine the teachings of Hohle with Zuk. Indeed, any potential combination of Hohle with Zuk would render the system of Hohle unsuitable for its intended purpose.

Hohle discloses methods and apparatus for a smart card system to integrate important travel related applications. *See Hohle*, Abstract. Further, Hohle is directed to updating data related to a card holder's travel information in the context of a distributed transaction system. *See id.*, Col. 1, ll. 8-11. Further, as stated in Hohle, the problem being addressed by the invention is that smart card efforts are fragmented and

the resulting benefit to consumers - particularly consumers who travel, has been quite minimal. *See id.*, Col. 2, ll. 8-11. In addition, Hohle addresses the issue of smart cards being incompatible. *See id.*, Col. 2, ll. 11-18. Further, Hohle is directed to providing a smart card system that securely and conveniently integrates important travel related applications overcoming the limitations of the prior art, in particular, in travel context such as airline, hotel, rental car, and payment related applications including specific applications with partnering organizations. *See id.*, Col. 2, ll. 22-34.

Zuk is directed at a method of initializing a smart card. *Zuk*, Col. 1 line 2. Zuk utilizes public key encryption methods to initialize the smart card, which is a one time event. Zuk explains that use of public key encryption for typical smart card applications is impractical.

> Public key techniques or algorithms, being computationally intensive have been considered too slow to execute and requiring too much memory in order to be practical for use on smart cards without additional specialised hardware. Most smart cards have very limited memory for both data and program storage, and employ microprocessors, such as 8 bit microprocessor, which are very slow compared with more powerful processors employed in personal computers and computer workstations. Many smart card applications require all of the program memory available on the card, and as much memory as possible for data, which *renders permanent hardware and software implementations of public key algorithms impractical. Zuk* Col. 2 ll. 15-27 (*emphasis added*).

Zuk also describes how the public key encryption applications and keys are erased from the smart card memory after initialization. Zuk states:

> The routines C1, C2 and C3 and m and r are erased by the routine C3 after the authentication key and the other data has been stored on the card 6 so as to advantageously allow the card 6 to use the memory space previously occupied by the routines and m and r. Therefore the card 6 which receives the initial secret data only needs to perform the public encryption part of the RSA algorithm and the memory used to execute this part is recovered after the secret data is received. *Zuk*, Col. 5 ll. 27-35.

Thus, Zuk describes a method of using public key encryption to perform the one-time method of smart card initialization. After the smart card is initialized, the public key encryption application and components are erased from the smart card,

because permanent implementation of public key algorithms are impractical in smart cards.

One of ordinary skill in the art would not be motivated to combine the teachings of Zuk with Hohle, because to do so would incorporate pubic key algorithms into a system that needs to have the ability to be continually updated with new user preferences. As stated in Zuk, the permanent use of public key algorithms in smart cards is impractical. The implementation of one time use of public key algorithms described in Zuk would render the system of Hohle unsuitable for its intended purpose, because Hohle requires the user to have the ability to access and update the various travel preferences. The system Hohle would be inoperable if the public key algorithms were erased from the smart card after use.

Therefore, claims 1, 2, 4-17, and 29-35 are believed to be allowable at least for the reasons that there is no motivation to combine the teachings of Hohle with Zuk. Indeed, Zuk states that use of public key algorithms in smart cards are impractical. There may be additional, independent, reasons that each of claims 1, 2, 4-17, and 29-35 is allowable over Hohle in combination with Zuk. For example, neither Hohle nor Zuk describes an RF communication channel. However, discussion of the independent reasons for allowability are unnecessary in light of the lack of motivation to combine.

Claim 21 recites a "method of establishing a secure communication link between a smart card and a central computer system remotely located from the smart card." The method includes "downloading communication link interface software to a processor from a remote *non-secure* computer system." (*emphasis added*). An example of this embodiment is provided in Applicant's Figure 1 and the associated description, where the local processor downloads an applet from the non-secure HTTP server.

In contrast, neither Hohle nor Murphy describes downloading software from a non-secure computer system. As conceded by the Examiner, Hohle fails to describe downloading communication link software. Murphy also fails to describe the claimed feature.

In contrast, Murphy, in figure 1 and the associated description, describes an interface with secure servers. The client terminal does not have any interface with a non-secure communication system and there is no description of software downloaded from a non-secure communication system. Thus, the combination of Hohle with Murphy fails to teach or suggest every claimed feature of claim 21.

Applicant respectfully requests reconsideration and allowance of claim 21, because Hohle and Murphy, either alone or in combination, fail to describe each and every feature of the claim.

Claim 22 includes "the secure data corresponds to secure data exchanged between the smart card communication device and the smart card through a radio frequency channel." Claim 22 also includes "exchanging the secure data with the central computer system through a communication network."

As noted earlier, Hohle fails to describe secure data exchanged through an RF channel. Murphy also fails to describe such a feature. Indeed, Murphy cannot utilize an RF communication channel to the card because the smart card is inserted into a 3.5 inch floppy drive for reading the card. *See, Murphy*, Col. 6 ll. 4-7.

Thus, Hohle and Murphy, either alone or in combination , fail to describe each and every feature of the claim. Applicant respectfully requests reconsideration and allowance of claim 22.

Claims 23-28 depend, either directly or indirectly from claim 22 and are believed to be allowable at least for the reasons that they depend from an allowable base claim. Applicant respectfully requests reconsideration and allowance of claims 22-28.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 858-350-6100.

Respectfully submitted,

Raymond B. Hom
Reg. No. 44,773

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 858-350-6100
Fax: 415-576-0300

RBH:jo
60428438 v1